On the Fundamental Structure of Galois Switching Functions

B. Benjauthrit
TDA Engineering

I. S. Reed
University of Southern California

It is shown that the fundamental structure of Galois switching functions follows naturally from that of Boolean switching functions. An expanded formula for deriving multinomial Galois switching functions is provided with illustrations of its application.

I. Introduction

Due to its simple and systematic properties, the Boolean field and its algebra have been applied successfully to binary-valued logic. Since the Galois or finite field is the natural extension of the Boolean field, more and more researchers have become interested in utilizing finite fields in the design of multivalued logics. It will be evident later that multivalued logic, using Galois field theory or algebra, is now as realizable as Boolean switching logic. This may be considered to be a consequence of the recent efforts of Menger (Ref. 1), Benjauthrit and Reed (Ref. 2), and Pradhan (Ref. 3). The second paper provided a systematic method of deriving any multinomial Galois switching functions via what is referred to as "Galois differences." The third paper furnished still another expansion for obtaining such switching functions.

Though both methods provide a systematic technique for deriving a unique Galois switching function from a given truth table description of the function, each requires tedious computation. Specifically, the first method often contains many redundant terms in its formulation, whereas the second method requires a great number of multiplications and additions. By some algebraic manipulations, an expanded formula is obtained which combines the best features of both methods. This formula enables one to compute the coefficients of the desired function more directly and probably with less effort.

II. Summary of Existing Results

Since most of the basic properties of Galois fields have been given in the literature, they will not be described here. Instead, use will be made of these properties as necessary and the reader will be directed to the appropriate references. Two basic theorems are now stated.

Let $q = p^n$ be the order or the number of field elements of Galois field $GF(q)$ whose field power is n and characteristic is a prime p. Denote the set of all nonzero field elements by $GF'(q)$. Also, let the symbol Σ_F signify the sum of all elements over F. Then, according to Ref. 2, one has the following theorem.

Theorem 1. For every function F: $GF(p^n)^m \rightarrow GF(p^n)$, there exists a unique function f: $\{0,1,\cdots,p^n - 1\} \rightarrow GF(p^n)$ such that

$$F(x_1,\cdots,x_m) = \sum f(k_1,\cdots,k_m)\, x_1^{k_1}\cdots x_m^{k_m}$$

where the function f is given by

$$f(\underline{0}) = F(\underline{0})$$

$$f(k_1,0,\cdots,0) = \underset{x_1^{k_1}}{\Delta} F(\underline{0}) = \sum_{GF'(p^n)} [F(\underline{0}) - F(\gamma_1,0,\cdots,0)]\,\gamma_1^{-k_1}$$

$$f(k_1,k_2,\cdots,0) = \underset{x_1^{k_1}x_2^{k_2}}{\Delta^{(2)}} F(\underline{0})$$

$$= \underset{GF'\ (p^n)}{\sum\sum} [F(\underline{0}) - F(0,\gamma_2,0,\cdots,0) - F(\gamma_1,0,0,\cdots,0) + F(\gamma_1,\gamma_2,0,\cdots,0)]\,\gamma_1^{-k_1}\gamma_2^{-k_2}$$

$$f(k_1,\cdots,k_m) = \underset{x_1^{k_1}\cdots x_m^{k_m}}{\Delta^{(m)}} F(\underline{0})$$

$$= \underset{GF'(p^n)}{\sum\overset{m}{\cdots}\sum} [F(\underline{0}) - F(0,\cdots,0,\gamma_m) - \cdots - F(\gamma_1,0,\cdots,0)$$

$$+ F(0,\cdots,0,\gamma_{m-1},\gamma_m) + \cdots + F(\gamma_1,\gamma_2,0,\cdots,0)$$

$$- \cdots (-1)^m F(\gamma_1,\cdots,\gamma_m)]\ \gamma_1^{-k_1}\cdots\gamma_m^{-k_m}$$

and

$$\underset{x_{i_1}\cdots x_{i_p}}{\Delta^{(p)}} F(\underline{0}) = \underset{x_{i_p}}{\Delta}\left[\underset{x_{i_1}\cdots x_{i_{p-1}}}{\Delta^{(p-1)}} F(\underline{0})\right], \text{ for } p = 1, 2, \cdots, m$$

The function $F(x_1, \cdots, x_m)$ has the following "power series" expansion:

$$F(x_1, \cdots, x_m) = F(\underline{0}) + \left[\underset{x_1}{\Delta} F(\underline{0}) \right] x_1 + \cdots + \left[\underset{x_m}{\Delta} F(\underline{0}) \right] x_m$$

$$+ \left[\underset{x_1^2}{\Delta} F(\underline{0}) \right] x_1^2 + \cdots + \left[\underset{x_m^2}{\Delta} F(\underline{0}) \right] x_m^2 + \cdots + \left[\underset{x_m^q}{\Delta} F(\underline{0}) \right] x_m^q$$

$$+ \left[\underset{x_1 x_2}{\Delta^{(2)}} F(\underline{0}) \right] x_1 x_2 + \cdots + \left[\underset{x_{m-1}^q x_m^q}{\Delta^{(2)}} F(\underline{0}) \right] x_{m-1}^q x_m^q$$

$$+ \left[\underset{x_1 \cdots x_m}{\Delta^{(m)}} F(\underline{0}) \right] x_1 \cdots x_m + \cdots + \left[\underset{x_1^q \cdots x_m^q}{\Delta^{(m)}} F(\underline{0}) \right] x_1^q \cdots x_m^q$$

where $F(0) \equiv F(0, \cdots, 0)$.

Now, from Ref. 3, the next theorem follows.

Theorem 2. Any function $F(x_1, \cdots, x_m)$ can be expressed as

$$F(x_1, \cdots, x_m) = \sum^{m} \cdots \sum_{GF(q)} g(\gamma_1, \cdots, \gamma_m) F(\gamma_1, \cdots, \gamma_m) \tag{1}$$

where

$$g(\gamma_1, \cdots, \gamma_m) = \prod_{i=1}^{m} [1 - (x_i - \gamma_i)^{q-1}], \quad \gamma \in GF(q) \tag{2}$$

Also from Ref. 3, we obtain the following lemmas:

Lemma 1. The sum of ith power of nonzero elements over the field $GF(q)$ is null for $0 < i < q - 1$ and unity for $i = q - 1$. Mathematically,

$$\sum_{GF'(q)} \alpha^i = \begin{cases} 0, & \text{for } 0 < i < q - 1 \quad \text{(3a)} \\ -1, & \text{for } i = q - 1 \quad \text{(3b)} \end{cases}$$

Note that Lemma 1 is not restricted to $q > 2$ here because, for $q = 2$, (3a) does not hold for $i \neq 0$ and thus only (3b) implies.

Lemma 2.

$$1 - (x - \gamma)^{q-1} = \begin{cases} 1 - x^{q-1}, & \gamma = 0 \\ 1 - \sum\limits_{i=0}^{q-1} (-1)^{q-1-i} \binom{q-1}{q-1-i} \gamma^{q-1-i} x^{i}, & \gamma \in GF'(q) \end{cases}$$

III. The Expanded Formula

For later use, a generalized version of Lemma 1 is first stated and proven.

Lemma 3. For any positive integer m,

$$\sum_{GF'(q)}^{m} \cdots \sum \gamma_1^{i_1} \cdots \gamma_m^{i_m} = \begin{cases} (-1)^m, & \text{for } i_1 = q-1, \cdots, i_m = q-1 \\ 0, & \text{otherwise} \end{cases}$$

Proof. The lemma follows directly from the factorizability property of the summation and by repeated applications of Lemma 1. For example, when $m = 2$, one has

$$\sum_{GF'(q)} \sum \gamma_1^{i_1} \gamma_2^{i_2} = \left[\sum_{GF'(q)} \gamma_1^{i_1}\right] \left[\sum_{GF'(q)} \gamma_2^{i_2}\right]$$

$$= \begin{cases} -\sum\limits_{GF'(q)} \gamma_2^{i_2} \; (\text{for } i_1 = q-1) = \begin{cases} 1, & i_2 = q-1 \\ 0, & \text{otherwise} \end{cases} \\ 0, \quad \text{otherwise} \end{cases}$$

Q.E.D.

The following two lemmas and their consequence are also useful.

Lemma 4. Let p be prime and $1 \leqslant i \leqslant p^n - 1$ for any integer $n \geqslant 1$. Then,

$$\binom{p^n}{i} \equiv 0 \bmod p \tag{4}$$

Proof. We shall prove the lemma by induction on n. For $n = 1$,

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!} = \frac{pk}{i!}, \text{ an integer}$$

This implies that $i!|pk$. But $i < p$ and, thus, the gcd$(i!, p) = 1$. Hence, $i!|k$ so that $\binom{p}{i} = p \cdot$ integer and relation (4) holds.

Hypothesize that relation (4) is true for n. We must now show that it is also true for $n + 1$. In so doing, express the polynomial $(1 + x)^{p^{n+1}}$ in two ways:

$$(1+x)^{p^{n+1}} = \sum_{i=0}^{p^{n+1}} \binom{p^{n+1}}{i} x^i \tag{5}$$

and

$$(1+x)^{p^{n+1}} = ((1+x)^{p^n})^p = \left(\sum_{j=0}^{p^n} \binom{p^n}{j} x^j\right)^p$$

$$= \sum_{j_1=0}^{p^n} \cdots \sum_{j_p=0}^{p^n} \binom{p^n}{j_1} \cdots \binom{p^n}{j_p} x^{j_1+\cdots+j_p}$$

$$= \sum_{i=0}^{p^{n+1}} x^i \sum_{j_1+\cdots+j_p=i} \cdots \sum \binom{p^n}{j_1} \cdots \binom{p^n}{j_p} \tag{6}$$

It follows that

$$\binom{p^{n+1}}{i} = \sum_{\substack{j_1+\cdots+j_p=i\\ 0 \leqslant j_\nu \leqslant p^n}} \cdots \sum \binom{p^n}{j_1} \cdots \binom{p^n}{j_p}, 0 \leqslant i \leqslant p^{n+1} \tag{7}$$

Let $1 \leqslant i \leqslant p^{n+1} - 1$. If $0 \leqslant j_\nu \leqslant p^n$ and

$$\sum_{\nu=1}^{p} j_\nu = i$$

then, some j_μ satisfies the condition $1 \leqslant j_\mu \leqslant p^n - 1$. By the induction hypothesis,

$$\binom{p^n}{j_\mu} \equiv 0 \bmod p$$

Then, each term in the sum of (7) is 0 mod p so that

$$\binom{p^{n+1}}{i} \equiv 0 \bmod p$$

On the other hand, suppose that all the j_ν are either 0 or p^n. Then, the product in (7) is 1. This can happen only if $i = ap^n$, where $1 \leqslant a \leqslant p - 1$; in this case, the number of such terms on the right side of (7) is $\binom{p}{a}$, a multiple of p, and thus (4) also follows.

Q.E.D.

Lemma 5. Let p be prime, and $0 \leqslant i \leqslant p^n - 1$ for any integer $n \geqslant 0$. Then,

$$\binom{p^n - 1}{i} \equiv (-1)^i \bmod p \tag{8}$$

Proof. It is trivial for the case $n = 0$. Let $n \geqslant 1$ and use induction on i. Relation (8) is obviously true for $i = 0$. By the Pascal triangle relationship, if $0 \leqslant i \leqslant p^n - 1$, then

$$\binom{p^n - 1}{i} + \binom{p^n - 1}{i+1} = \binom{p^n}{i+1}$$

By Lemma 4, the right side is 0 mod p, and the induction hypothesis is (8). Hence, relation (8) is true for the case i replaced by $i + 1$.

Q.E.D.

By multiplying both sides of relation (8) in Lemma 5 by the quantity $(-1)^{p^{n-1-i}}$ and noting the identity $+ \equiv -$ *for* $p = 2$, one obtains the following corollary.

Corollary 1. Let p be prime and $0 \leqslant i \leqslant p^n - 1$ for any integer $n \geqslant 0$. Then

$$(-1)^{p^n-1-i} \binom{p^n - 1}{i} \equiv 1 \bmod p$$

Since $\gamma^{q-1} = 1, \gamma \in GF'(q)$, and with Corollary 1, Lemma 2 yields:

Lemma 6.

$$\prod_{i=1}^{m} [1 - (x_i - \gamma_i)^{q-1}] = \begin{cases} \prod_{i=1}^{m} [1 - x_i^{q-1}], \ \gamma = 0 & \text{(9a)} \\ \prod_{i=1}^{m} -\sum_{j=1}^{q-1} \gamma_i^{-j} x_i^j, \ \gamma \in GF'(q) & \text{(9b)} \end{cases}$$

With the above theorems and lemmas, one can now state and prove the following expanded formula.

Theorem 3. For every function F: $GF(q)^m \to GF(q)$, there exists a unique function f: $[1, \cdots, q-1] \to GF(q)$ such that

$$F(x_1, \cdots, x_m) = \begin{cases} \overset{m}{\underset{GF(q)}{\sum \cdots \sum}} \; g(\gamma_1, \cdots, \gamma_m) F(\gamma_1, \cdots, \gamma_m) \\ \sum_{k_1=0}^{q-1} \cdots \sum_{k_m=0}^{q-1} f(k_1, \cdots, k_m) x_1^{k_1} \cdots x_m^{k_m} \end{cases}$$

where

i) $$g(\gamma_1, \cdots, \gamma_m) = \prod_{i=1}^{m} [1 - (x_i - \gamma_i)^{q-1}]$$

$$= \begin{cases} 1 + \sum_{i=1}^{m} (-1)^i \sum_{j_1 < j_2 < \cdots < j_i} x_{j_1}^{q-1} x_{j_2}^{q-1} \cdots x_{j_i}^{q-1}, \quad \gamma = 0, 1 \leqslant j_l \leqslant m \\ \prod_{i=1}^{m} -\sum_{j=1}^{q-1} \gamma_i^{-j} x_i^j, \quad \gamma \in GF'(q) \end{cases} \tag{10a}$$

and

$$g(\gamma_1, \cdots, \gamma_k, 0, \cdots, 0) = \left[\prod_{i=1}^{k} -\sum_{j=1}^{q-1} \gamma_i^{-j} x_i^j \right] \left[1 + \sum_{i=1}^{m-k} (-1)^i \sum_{j_1 < j_2 < \cdots < j_i} x_{j_1}^{q-1} x_{j_2}^{q-1} \cdots x_{j_i}^{q-1} \right] \tag{10b}$$

for any k, $1 \leqslant k \leqslant m$, $\gamma \in GF'(q)$, and $k < j_l \leqslant m$

ii) $$f(0, \cdots, 0) = F(0, \cdots, 0)$$

$$f(k_1, 0, \cdots, 0) = -\sum_{GF'(q)} F(\gamma_1, 0, \cdots, 0) \gamma_1^{-k_1}$$

$$\vdots$$

$$f(q-1, 0, \cdots, 0) = -\sum_{GF(q)} F(\gamma_1, 0, \cdots, 0)$$

$$\vdots$$

$$f(k_1, k_2, 0, \cdots, 0) = \underset{GF'(q)}{\sum\sum} F(\gamma_1, \gamma_2, 0, \cdots, 0)\, \gamma_1^{-k_1} \gamma_2^{-k_2}$$

$$\vdots$$

$$f(q-1, q-1, 0, \cdots, 0) = \underset{GF(q)}{\sum\sum} F(\gamma_1, \gamma_2, 0, \cdots, 0)$$

$$\vdots$$

$$f(k_1, \cdots, k_i, 0, \cdots, 0) = (-1)^i \underset{GF'(q)}{\sum \overset{i}{\cdots} \sum} F(\gamma_1, \cdots, \gamma_i, 0, \cdots, 0)\, \gamma_1^{-k_1} \cdots \gamma_i^{-k_i}$$

$$\vdots$$

$$f(q-1, \cdots, q-1, 0, \cdots, 0) = (-1)^i \underset{GF\,(q)}{\sum \overset{i}{\cdots} \sum} F(\gamma_1, \cdots, \gamma_i, 0, \cdots, 0)$$

$$\vdots$$

$$f(k_1, \cdots, k_m) = (-1)^m \underset{GF'(q)}{\sum \overset{m}{\cdots} \sum} F(\gamma_1, \cdots, \gamma_m)\, \gamma_1^{-k_1} \cdots \gamma_m^{-k_m}$$

$$\vdots$$

$$f(q-1, k_2, \cdots, k_m) = (-1)^m \left[\underset{GF'(q)}{\sum \overset{m-1}{\cdots} \sum} F(0, \gamma_2, \cdots, \gamma_m)\, \gamma_2^{-k_2} \cdots \gamma_m^{-k_m} \right.$$

$$\left. + \underset{GF'(q)}{\sum \overset{m}{\cdots} \sum} F(\gamma_1, \cdots, \gamma_m)\, \gamma_2^{-k_2} \cdots \gamma_m^{-k_m} \right]$$

$$\vdots$$

$$f(q-1, q-1, k_3, \cdots, k_m) = (-1)^m \left[\underset{GF'(q)}{\sum \overset{m-2}{\cdots} \sum} F(0, 0, \gamma_3, \cdots, \gamma_m)\, \gamma_3^{-k_3} \cdots \gamma_m^{-k_m} \right.$$

$$+ \sum\limits^{m-1}\cdots\sum\limits_{GF'(q)} F(0, \gamma_2, \cdots, \gamma_m)\gamma_3^{-k_3}\cdots\gamma_m^{-k_m}$$

$$+ \sum\limits^{m-1}\cdots\sum\limits_{GF'(q)} F(\gamma_1, 0, \gamma_3, \cdots, \gamma_m)\gamma_3^{-k_3}\cdots\gamma_m^{-k_m}$$

$$\left. + \sum\limits^{m}\cdots\sum\limits_{GF'(q)} F(\gamma_1, \cdots, \gamma_m)\gamma_3^{-k_3}\cdots\gamma_m^{-k_m}\right]$$

$$\vdots$$

$$f(q-1, \cdots, q-1, k_{i+1}, \cdots, k_m) = (-1)^m \left[\sum\limits^{m-i}\cdots\sum\limits_{GF'(q)} F(0, \cdots, 0, \gamma_{i+1}, \cdots, \gamma_m)\gamma_{i+1}^{-k_{i+1}}\cdots\gamma_m^{-k_m}\right.$$

$$+ \sum\limits^{m-i-1}\cdots\sum\limits_{GF'(q)} F(0, \cdots, 0, \gamma_i, \cdots, \gamma_m)\gamma_{i+1}^{-k_{i+1}}\cdots\gamma_m^{-k_m} + \cdots$$

$$+ \sum\limits^{m-i-1}\cdots\sum\limits_{GF'(q)} F(\gamma_1, 0, \cdots, 0, \gamma_{i+1}, \cdots, \gamma_m)\gamma_{i+1}^{-k_{i+1}}\cdots\gamma_m^{-k_m} + \cdots$$

$$+ \sum\limits^{m-i-2}\cdots\sum\limits_{GF'(q)} F(0, \cdots, 0, \gamma_{i-1}, \cdots, \gamma_m)\gamma_{i+1}^{-k_{i+1}}\cdots\gamma_m^{-k_m} + \cdots$$

$$+ \sum\limits^{m-i-2}\cdots\sum\limits_{GF'(q)} F(\gamma_1, \gamma_2, 0, \cdots, 0, \gamma_{i+1}, \cdots, \gamma_m)\gamma_{i+1}^{-k_{i+1}}\cdots\gamma_m^{-k_m} + \cdots$$

$$\left. + \sum\limits^{m}\cdots\sum\limits_{GF'(q)} F(\gamma_1, \cdots, \gamma_m)\gamma_{i+1}^{-k_{i+1}}\cdots\gamma_m^{-k_m}\right]$$

$$f(q-1, \cdots, q-1) = (-1)^m \sum\limits^{m}\cdots\sum\limits_{GF\,(q)} F(\gamma_1, \cdots, \gamma_m) \tag{10c}$$

In words, for those coefficients containing no $q - 1$ as their arguments, we simply expand the function around the point(s) being considered. For any coefficients containing $q - 1$ as its arguments, the function's "initial value(s)" must be included in the expansion. Finally, the last coefficient $f(q-1, \cdots, q-1)$ includes all points, i.e., all function output values, in its expansion.

Proof.

i) The result follows directly from Theorem 2 and Lemma 6.

ii) Coefficients (10c) can be derived from either Theorem 1 or Theorem 2. However, since these two theorems have been independently proven to be correct (Refs. 2 and 3), the uniqueness of Lagrange's expansion of m-variable functions (Ref. 4) guarantees that they both lead to the same unique function. For simplicity, Theorem 1 will be employed here, together with Lemma 1 or Lemma 3.

For $m = 1$,

$$f(k_1) = \sum_{GF'(q)} [F(0) - F(\gamma_1)] \, \gamma_1^{-k_1}$$

$$= F(0) \sum_{GF'(q)} \gamma_1^{-k_1} - \sum_{GF'(q)} F(\gamma_1) \gamma_1^{-k_1}$$

$$= \begin{cases} - \sum\limits_{GF'(q)} F(\gamma_1) \gamma_1^{-k_1}, 0 < k_1 < q - 1 \\ - \sum\limits_{GF(q)} F(\gamma_1), k_1 = q - 1 \end{cases}$$

For $m = 2$,

$$f(k_1, k_2) = \sum\sum_{GF'(q)} [F(0,0) - F(0,\gamma_2) - F(\gamma_1, 0) + F(\gamma_1, \gamma_2)] \, \gamma_1^{-k_1} \gamma_2^{-k_2}$$

$$= F(0,0) \left[\sum_{GF'(q)} \gamma_1^{-k_1} \right] \left[\sum_{GF'(q)} \gamma_2^{-k_2} \right]$$

$$- \left[\sum_{GF'(q)} \gamma_1^{-k_1} \right] \left[\sum_{GF'(q)} F(0, \gamma_2) \gamma_2^{-k_2} \right]$$

$$- \left[\sum_{GF'(q)} \gamma_2^{-k_2} \right] \left[\sum_{GF'(q)} F(\gamma_1, 0) \gamma_1^{-k_1} \right]$$

$$+ \sum\sum_{GF'(q)} F(\gamma_1, \gamma_2) \gamma_1^{-k_1} \gamma_2^{-k_2}$$

Therefore,

$$f(k_1, k_2) = \begin{cases} \displaystyle\sum\sum_{GF'(q)} F(\gamma_1, \gamma_2)\gamma_1^{-k_1}\gamma_2^{-k_2}, 0 < k_1, k_2 < q - 1 \\[2ex] \displaystyle\sum_{GF'(q)} F(0, \gamma_2)\gamma_2^{-k_2} + \sum\sum_{GF'(q)} F(\gamma_1, \gamma_2)\gamma_2^{-k_2}, k_1 = q - 1, 0 < k_2 < q - 1 \\[2ex] \displaystyle\sum_{GF'(q)} F(\gamma_1, 0)\gamma_1^{-k_1} + \sum\sum_{GF'(q)} F(\gamma_1, \gamma_2)\gamma_1^{-k_1}, 0 < k_1 < q - 1, k_2 = q - 1 \\[2ex] \displaystyle\sum\sum_{GF\ (q)} F(\gamma_1, \gamma_2), k_1 = k_2 = q - 1 \end{cases}$$

Now, assuming it is true for the m case, we shall show that the $m + 1$ case follows:

$$f(k_1, \cdots, k_m, k_{m+1}) = (-1)^{m+1} \overset{m+1}{\sum\cdots\sum_{GF'(q)}} F(\gamma_1, \cdots, \gamma_m, \gamma_{m+1})\gamma_1^{-k_1} \cdots \gamma_m^{-k_m}\gamma_{m+1}^{-k_{m+1}}$$

$$\begin{aligned} f(q-1, k_2, \cdots, k_m, k_{m+1}) = (-1)^{m+1} &\Bigg[\overset{m+1-1}{\sum\cdots\sum_{GF'(q)}} F(0, \gamma_2, \cdots, \gamma_m, \gamma_{m+1})\gamma_2^{-k_2} \cdots \gamma_m^{-k_m}\gamma_{m+1}^{-k_{m+1}} \\ &+ \overset{m+1}{\sum\cdots\sum_{GF'(q)}} F(\gamma_1, \cdots, \gamma_m, \gamma_{m+1})\gamma_2^{-k_2} \cdots \gamma_m^{-k_m}\gamma_{m+1}^{-k_{m+1}} \Bigg] \end{aligned}$$

$$\vdots$$

$$\begin{aligned} f(q-1, q-1, k_3, \cdots, k_m, k_{m+1}) = (-1)^{m+1} &\Bigg[\overset{m+1-2}{\sum\cdots\sum_{GF'(q)}} F(0,0, \gamma_3, \cdots, \gamma_m, \gamma_{m+1})\gamma_3^{-k_3} \cdots \gamma_m^{-k_m}\gamma_{m+1}^{-k_{m+1}} \\ &+ \cdots + \overset{m+1}{\sum\cdots\sum_{GF'(q)}} F(\gamma_1, \cdots, \gamma_m, \gamma_{m+1})\gamma_3^{-k_3} \cdots \gamma_m^{-k_m}\gamma_{m+1}^{-k_{m+1}} \Bigg] \end{aligned}$$

$$\vdots$$

$$f(q-1, \cdots, q-1) = (-1)^{m+1} \overset{m+1}{\sum\cdots\sum_{GF'(q)}} F(\gamma_1, \cdots, \gamma_m, \gamma_{m+1})$$

which are exactly the coefficients (10c) when $m + 1$ is redefined as m. This completes the proof.

It is not difficult to show that a similar proof of Theorem 3 can also be obtained from Theorem 2, especially for case $m = 1$. For case $m = 2$, from Theorem 2 and Lemma 6, one has

$$F(x_1, x_2) = \sum\sum_{GF(q)} g(\gamma_1, \gamma_2) F(\gamma_1, \gamma_2)$$

$$= [1 - x_1^{q-1} - x_2^{q-1} + x_1^{q-1}\, x_2^{q-1}]\ F(0,0)$$

$$+ [1 - x_1^{q-1}] \sum_{GF'(q)} \left[- \sum_{k_2=1}^{q-1} \gamma_2^{-k_2} x_2^{k_2} \right] F(0, \gamma_2)$$

$$+ [1 - x_2^{q-1}] \sum_{GF'(q)} \left[- \sum_{k_1=1}^{q-1} \gamma_1^{-k_1} x_1^{k_1} \right] F(\gamma_1, 0)$$

$$+ \sum\sum_{GF'(q)} \left[- \sum_{k_1=1}^{q-1} \gamma_1^{-k_1} x_1^{k_1} \right] \left[- \sum_{k_2=1}^{q-1} \gamma_2^{-k_2} x_2^{k_2} \right] F(\gamma_1, \gamma_2)$$

Again, using basic properties of the summation and with some simple manipulation, one obtains

$$F(x_1, x_2) = F(0,0) + \sum_{k_1=1}^{q-2} \left[- \sum_{GF'(q)} F(\gamma_1, 0) \gamma_1^{-k_1} \right] x_1^{k_1} - \left[\sum_{GF(q)} F(\gamma_1, 0) \right] x_1^{q-1}$$

$$+ \sum_{k_2=1}^{q-2} \left[- \sum_{GF'(q)} F(0, \gamma_2) \gamma_2^{-k_2} \right] x_2^{k_2} - \left[\sum_{GF(q)} F(0, \gamma_2) \right] x_2^{q-1}$$

$$+ \sum_{k_1=1}^{q-2} \sum_{k_2=1}^{q-2} \left[\sum\sum_{GF'(q)} F(\gamma_1, \gamma_2) \gamma_1^{-k_1} \gamma_2^{-k_2} \right] x_1^{k_1} x_2^{k_2}$$

$$+ \cdots + \left[F(0,0) + \sum_{GF'(q)} F(0, \gamma_2) + \sum_{GF'(q)} F(\gamma_1, 0) + \sum\sum_{GF'(q)} F(\gamma_1, \gamma_2) \right] x_1^{q-1} x_2^{q-1}$$

which contains exactly the coefficients given in (10c). To complete the proof, an induction on m may be accomplished similar to the previous case.

Q.E.D.

IV. Examples

We now provide two examples to illustrate the effectiveness of Theorem 3. For convenience and to the point, let us consider Example 1 described in Ref. 3. By partitioning as follows,

$$(y^1, y^2) = y$$

$$(x^1, x^2) = x_1$$

$$(x^3, x^4) = x_2$$

$$(x^5, x^6) = x_3$$

and representing (0, 0) by 0, (0, 1) by 1, (1, 0) by α, and (1, 1) by β, the given six-input two-output variable function is represented as shown in Table 1; the all-zero rows are omitted here.

Using Theorem 2 and observing that rows 1, 2, 7 and rows 3, 4, 5, 6 have the values of x_2, x_3, y and x_1, x_2, respectively, in common, we obtain

$$\begin{aligned} y &= \beta\,[1-(x_2-\beta)^3]\,[1-x_3^3]\,\{[1-x_1^3]+[1-(x_1-1)^3]+[1-(x_1-\beta)^3]\,\} \\ &\quad + [1-(x_1-\alpha)^3]\,[1-(x_2-\beta)^3]\,\{\alpha\,[1-x_3^3]\,+[1-(x_3-1)^3]+\,[1-(x_3-\alpha)^3]+[1-(x_3-\beta)^3]\,\} \end{aligned}$$

Making use of Lemma 2 and noting the identity $+ \equiv -$, y can be simplified as

$$\begin{aligned} y &= x_2 + \alpha x_2^2 + \beta x_2^3 + x_1 x_2 + \alpha x_1 x_2^2 + \beta x_1 x_2^3 + \beta x_1^2 x_2 + x_1^2 x_2^2 \\ &\quad + \alpha x_1^2 x_2^3 + \alpha x_1^3 x_2 + \beta x_1^3 x_2^2 + x_1^3 x_2^3 + x_2 x_3^3 + \alpha x_2^2 x_3^3 + \beta x_2^3 x_3^3 \end{aligned}$$

Now by applying Theorem 3 and Table 2, we can verify the above result termwise as follows:

$$f(0,1,0) = \sum_{GF'(4)} F(0,\gamma_2,0)\,\gamma_2^{-1} = 0+0+\beta\cdot\alpha = 1$$

$$f(0,2,0) = \sum_{GF'(4)} F(0,\gamma_2,0)\,\gamma_2^{-2} = 0+0+\beta\cdot\beta = \alpha$$

$$\vdots$$

$$f(1,1,0) = \sum_{GF'(4)} F(\gamma_1,\gamma_2,0)\,\gamma_1^{-1}\,\gamma_2^{-1} = 0+0+\alpha\cdot\beta+0+\alpha\cdot\beta\cdot\alpha+0+\beta\cdot\alpha\cdot\alpha = 1$$

$$\vdots$$

$$f(3,3,0) = \sum_{GF(4)} F(\gamma_1, \gamma_2, 0) = 0+0+0+\beta+0+0+0+\beta+0+0+0+\alpha+0+0+0+\beta = 1$$

$$\vdots$$

$$f(0,3,3) = \sum_{GF(4)} F(0, \gamma_2, \gamma_3) = 0+\cdots+0+\beta+0+0+0 = \beta$$

$$\vdots$$

$$f(3,3,2) = \sum_{GF'(4)} F(0,0,\gamma_3)\gamma_3^{-2} + \sum\sum_{GF'(4)} F(0,\gamma_2,\gamma_3)\gamma_3^{-2} + \sum\sum_{GF'(4)} F(\gamma_1, 0, \gamma_3)\gamma_3^{-2}$$

$$+ \sum\sum\sum_{GF'(4)} F(\gamma_1, \gamma_2, \gamma_3)\gamma_3^{-2}$$

$$= [0+0+0] + [(0+\cdots+0+1+0+0+0) + (0+\cdots+0+1+0+0+0)\alpha + (0+\cdots+0+1+0+0+0)\beta] = 0$$

As another example, consider the four-input two-output specification given in Table 2 of Ref. 2. Using the same representation for $GF(3^2)$,

$$0 = 00,\ 1 = \alpha^0 = 10,\ \alpha = 01,\ \alpha^2 = 12,\ \alpha^3 = 22,\ \alpha^4 = 20,\ \alpha^5 = 02,\ \alpha^6 = 21,\ \alpha^7 = 11$$

and the same partition

$$x_1 = \{u_1, u_2\}, x_2 = \{u_3, u_4\}, \text{and } F = \{\nu_1, \nu_2\};$$

the truth table is obtained as given in Table 3.

Employing Theorem 3 here and Table 1 in Ref. 2, Eq. (16) of Ref. 2 may be verified term by term as follows:

$$f(1,0) = -\sum_{GF'(9)} F(\gamma_1, 0)\gamma_1^{-1} = -\alpha - \cdots - \alpha = -\alpha - \alpha = -\alpha^5 = \alpha$$

$$f(0,3) = -\sum_{GF'(9)} F(0, \gamma_2)\gamma_2^{-3} = -1 - \cdots - 1 = -1 - 1 = -\alpha^4 = 1$$

$$f(1,1) = \sum\sum_{GF'(9)} F(\gamma_1, \gamma_2)\gamma_1^{-1}\gamma_2^{-1} = 1$$

$$f(5,7) = \sum\sum_{GF'(9)} F(\gamma_1, \gamma_2)\gamma_1^{-5}\gamma_2^{-7} = 1$$

The sum of the output functions F results in

$$f(8,8) = \sum_{GF(9)}\sum F(\gamma_1, \gamma_2) = 1$$

The remaining 75 terms can be similarly verified to be all zeros. Hence,

$$f(x_1, x_2) = \alpha x_1 + x_2^3 + x_1 x_2 + x_1^5 x_2^7 + x_1^8 x_2^8$$

It is evident that employing either Theorem 1 or Theorem 2 to compute $F(x_1, x_2)$ of the above example would be tedious. This is especially true for Theorem 2.

Observe that Theorem 3 always requires a fixed number of computations; i.e., q^m computations for m variables over $GF(q)$. For truth tables whose rows contain a great number of zeros, the technique of Theorem 2 is no worse than that of Theorem 3; in fact, it is even better at times. However, for large m and large number of nonzero elements in the truth table, the advantage of Theorem 3 can truly be appreciated. The advantages and disadvantages of Theorem 3 over Theorems 1 and 2 are a subject of further investigation. But, for now, it is obvious that the technique provided in Theorem 3 is suitable both for hand and computer calculations.

V. Conclusion

Any Galois switching function can be expressed as the sum of minterms with a set of uniquely defined coefficients, or it can be expressed as the sum of its output-valued functions with also another set of uniquely defined coefficients. From these two approaches, we have derived an expanded version of the two methods. With this expanded formula, the function can be obtained more simply and directly from its given table of description. The novelty of the technique is illustrated by example.

Acknowledgments

The authors would like to thank Mr. B. D. L. Mulhall and Dr. J. S. L. Wong for their early support and encouragement in the research that led to this paper. Thanks are also due to Dr. C. A. Greenhall for his assistance on mathematical proofs.

References

1. Menger, K. S., Jr., "A Transform for Logic Networks," *IEEE Trans. Computers*, Vol. C-18, pp. 241-251, Mar. 1969.
2. Benjauthrit, B., and Reed, I. S., "Galois Switching Functions and Their Applications," in *The Deep Space Network Progress Report 42-27*, pp. 68-80, Jet Propulsion Laboratory, Pasadena, Calif., June 15, 1975.
3. Pradhan, D. K., *Structure and Minimization of Finite Field Functions*, Dept. of Computer Science, University of Saskatchewan, Regina, Saskatchewan, Feb. 1975.
4. Van der Waerden, B. L., *Algebra*, Vol. I, Federick Unger Publishing, 1966.

Table 1. Truth table of six-input two-output variable function

Row	x_1	x_2	x_3	y
	⋮	⋮	⋮	⋮
1	0	β	0	β
	⋮	⋮	⋮	⋮
2	1	β	0	β
	⋮	⋮	⋮	⋮
3	α	β	0	α
4	α	β	1	1
5	α	β	α	1
6	α	β	β	1
	⋮	⋮	⋮	⋮
7	β	β	0	β
	⋮	⋮	⋮	⋮

Table 2. Galois field operations

Addition over $GF(4)$					Multiplication over $GF(4)$				
+	0	1	α	β	.	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Table 3. An input-output truth table

x_1	x_2	F	x_1	x_2	F	x_1	x_2	F	x_1	x_2	F
0	0	0	α^5	α^5	α^7	α^7	α^7	0	α^4	α^4	α^3
0	α	α^3	α^5	1	α^7	α^7	α^2	1	α^4	α^6	α^6
0	α^5	α^7	α^5	α^7	α^5	α^7	α^4	1	α^4	α^3	α^3
0	1	1	α^5	α^2	α^7	α^7	α^6	0	α^6	0	α^7
0	α^7	α^5	α^5	α^4	α^6	α^7	α^3	1	α^6	α	α^4
0	α^2	α^6	α^5	α^6	α^6	α^2	0	α^3	α^6	α^5	α^3
0	α^4	α^4	α^5	α^2	0	α^2	α	α^7	α^6	1	1
0	α^6	α^2	1	0	α	α^2	α^5	α^4	α^6	α^7	0
0	α^3	α	1	α	α^2	α^2	1	0	α^6	α^2	α^2
α	0	α^2	1	α^5	1	α^2	α^7	α^6	α^6	α^4	α^5
α	α	1	1	1	α^7	α^2	α^2	α^4	α^6	α^6	0
α	α^5	α	1	α^7	α^3	α^2	α^4	α	α^6	α^3	α^2
α	1	α^5	1	α^2	α^5	α^2	α^6	α^7	α^3	0	α^4
α	α^7	α^3	1	α^4	α^7	α^2	α^3	1	α^3	α	0
α	α^2	α^6	1	α^6	α^4	α^4	0	α^5	α^3	α^5	0
α	α^4	α^2	1	α^3	0	α^4	α	α^3	α^3	1	1
α	α^6	α^4	α^7	0	1	α^4	α^5	α^5	α^3	α^7	α^6
α	α^3	α^3	α^7	α	α	α^4	1	α^5	α^3	α^2	α^3
α^5	0	α^6	α^7	α^5	α^2	α^4	α^7	α^5	α^3	α^4	α^4
α^5	α	α^6	α^7	1	0	α^4	α^2	0	α^3	α^6	α^7
									α^3	α^3	α^2